COMPUTER SECURITY OF GRANT MANAGEMENT AND PAYMENT SYSTEMS

Federal Transit Administration

Report Number: FI-2003-093

Date Issued: September 30, 2003

Memorandum

U.S. Department of
Transportation
Office of the Secretary
of Transportation
Office of Inspector General

Subject: ACTION: Report on Computer Security of Grant Management and Payment Systems, Federal Transit Administration
FI-2003-093

Date: September 30, 2003

From: Alexis M. Stefani
Principal Assistant Inspector General
for Auditing and Evaluation

Reply to
Attn. of: JA-20

To: Chief Information Officer
Federal Transit Administration

Associate Administrator for Budget and Policy
Federal Transit Administration

This audit report transmits the results of a computer security audit over three Federal Transit Administration (FTA) systems that support the grant administration and payment process. The audit was conducted by KPMG LLP of Washington, D.C. (KPMG), under contract to the Office of Inspector General (OIG). KPMG evaluated controls over the Transportation Electronic Award Management System (TEAM), Electronic Clearing House Operation System (ECHO), and Delphi Online Transaction System (DOTS).

The integrity of these systems is important because they are used to approve, monitor, and pay over $7 billion of annual FTA and Federal Aviation Administration grants. To illustrate, the ability of the TEAM and ECHO systems to process and pay grants in a timely manner is essential to ensuring compliance with the Cash Management Improvement Act, which requires Federal agencies to make timely fund transfers and grant awards. Additionally, the systems help ensure that sufficient funds are available to cover the grants in accordance with the Anti-Deficiency Act principles and that the actual amount paid does not exceed the total of the grant award.

This audit focused on entity-wide security program planning and management, access controls, network vulnerabilities, application software development and change controls, system software controls, segregation of duties, and service continuity. The audit was performed from May to July 2003.

We performed a quality assurance review of the KPMG audit work to determine compliance with applicable standards. These standards include Government Auditing Standards prescribed by the Comptroller General of the United States and the Federal Information Systems Controls Audit Manual (FISCAM) developed by the General Accounting Office. We agree with KPMG's findings and recommendations and, in our opinion, the audit work performed by KPMG complied with auditing standards. The scope and methodology of our review are discussed in Exhibit A. KPMG's audit report is provided as Exhibit B.

RESULTS

Computer security weaknesses exist in FTA's grant management and payment systems. Specifically, DOTS, ECHO, and TEAM have security vulnerabilities in security planning and management, access controls, change controls, and business continuity planning. FTA generally concurred with the findings and recommendations and has initiated corrective actions.

Security Planning and Management

- Information technology security planning and management is the foundation for establishing adequate system security, and the certification and accreditation review is key to ensuring the adequacy of the system security. KPMG found that FTA did not properly address certification and accreditation requirements. For example, FTA did not perform a security test before certifying and accrediting TEAM. KPMG also found that risk assessments and security plans were incomplete or not thorough enough for ECHO, DOTS, and TEAM. For example, the TEAM risk assessment did not include the possibility for common high risk threats such as computer hacking or malicious software attacks. FTA agreed to improve security planning and management by properly addressing certification and accreditation requirements, including completion of security testing, risk assessments, and security plans.

- KPMG also found inadequate background checks for all 10 financial system contractor employees it sampled, and for 1 of the 5 FTA employees it sampled. These individuals occupy sensitive positions for operating and maintaining mission critical systems but did not receive the proper level of background checks as required by DOT policy. For example, one system programmer was required to have a full Background Investigation but instead only received a low level fingerprint check. FTA agreed to perform background checks on all required contractor and FTA employees.

Access Controls

- Weaknesses exist in the process for granting, monitoring, and terminating user access to FTA financial systems. KPMG found that 9 of the 22 employees who were terminated during fiscal year 2003 still had access to TEAM as of July 2003. Of the remaining 13, access for 8 employees was not removed timely, allowing them system access for up to 4 months after termination. KPMG also found that access request forms and security agreements (Rules of Behavior) were not completed or adequately enforced. For example, only three of seven DOTS users sampled had completed user access request forms, and only two of seven DOTS users sampled had signed the security agreements. As a result, FTA financial systems are potentially vulnerable to unauthorized use, and management may not be able to hold individuals accountable for security breaches. Upon notice, FTA immediately removed system access for the nine TEAM users terminated and agreed to require Rules of Behavior to be signed for all users.

- KPMG's review identified five high and seven medium vulnerabilities in TEAM and DOTS.[1] As a result, these systems were vulnerable to attacks by DOT employees and contractors. These vulnerabilities existed because FTA did not install software patches provided by manufacturers or reconfigure existing software settings. FTA corrected these vulnerabilities identified during the audit.

- Physical access to the DOTS and ECHO data center is not adequately controlled because FTA did not maintain a current list of all those who had access to the data center nor had it periodically changed the combination to the lock on the door. FTA agreed to maintain a current list of all employees and periodically change the combination to the lock on the door.

System Change Control

- KPMG found that the ECHO system administrator was performing all aspects of the system change control process, from programming the change to implementing the change on the production computer, with no management oversight. There is also a lack of documented procedures for performing

[1] High vulnerabilities may provide an attacker with immediate access into the computer system, such as allowing execution of remote commands. Medium vulnerabilities may provide an attacker with useful information, such as password files, to compromise DOT computers.

technical system maintenance work. This results in a "key person dependency" on the current system administrator and could lead to unauthorized software changes if compensating controls are not established. FTA agreed to increase management oversight of and develop documented procedures for ECHO technical maintenance.

- DOTS and ECHO system software changes were not documented. For example, there was no documentation of test plans, test results, or user approval for changes made in the systems. As a result, management has no assurance that only authorized, and properly tested, system changes were made. FTA agreed to document DOTS and ECHO system software changes.

Disaster Recovery and Business Continuity Planning

- FTA has not conducted a business impact analysis, the fundamental first step in planning for contingencies, for these three systems. As a result, FTA does not know how long it could perform grant operations without computer system support. FTA cannot properly plan or test for a disaster without this analysis. FTA has agreed to conduct a business impact analysis for ECHO, DOTS, and TEAM.

- The existing contingency plans for ECHO and DOTS are not adequate to ensure continued operations in case of a disaster. The recovery processing site is not properly equipped and has never been tested. Also, the distance between the primary and recovery processing sites is only 25 miles, which may not be adequate separation in case of a large scale disaster. In addition, there are not adequately detailed procedures or trained backup personnel for disaster recovery operations. FTA has agreed to perform disaster recovery testing for ECHO and DOTS.

RECOMMENDATIONS

KPMG provided detailed recommendations to FTA management, which are included in Exhibit B. While we are not making any additional recommendations, in our opinion, the following are key action items that FTA officials should implement on a priority basis.

1. Test and evaluate security controls in TEAM and develop more comprehensive risk assessments and security plans for all three systems.

2. Complete the appropriate background checks on the Federal and contractor employees KPMG identified.

3. Develop procedures for granting, removing, and periodically revalidating user access, and enforce use of access request forms and security agreements (Rules of Behavior) before granting system access.

4. Regularly scan FTA financial system computers for vulnerabilities and timely install software patches provided by manufacturers or reconfigure software settings.

5. Enhance physical access controls over the ECHO and DOTS computer room by maintaining a list of individuals authorized to enter the data center and changing the combination to the lock on a periodic basis.

6. Increase management oversight of, and develop documented procedures for, ECHO system maintenance work.

7. Require that test plans, test results, and user approvals for ECHO and DOTS system changes be documented.

8. Enhance the contingency plans with a business impact analysis and detailed disaster recovery procedures including personnel roles and emergency notification for all three systems.

9. Test disaster recovery processes for ECHO and DOTS, and determine whether the recovery site is distant enough to ensure continued operations in case of large scale disasters.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On September 29, 2003, FTA provided comments (see Appendix) to our September 24, 2003 draft report. FTA concurred with all nine recommendations but needs clarify its response to recommendations 1, 8, and 9. Further, while FTA indicated for some of the recommendations that actions would be initiated or completed in fiscal years 2004 or 2005, we request that more specific action completion dates be provided.

Regarding recommendation 1, FTA has agreed to perform comprehensive risk assessments and update the security plans for all three systems. The response provides a commitment to perform a security test and evaluation for ECHO and DOTS. However, the reply does not address the need to test and evaluate security controls in TEAM and we request that FTA provide us its plans for testing TEAM. Further, based on the criticality of this requirement, we suggest that FTA complete this management action during fiscal year 2004.

In response to recommendation 8, FTA agreed with our recommendation to enhance the contingency plan of TEAM by performing a business impact analysis and including roles and emergency notification procedures. However, while FTA committed to developing step-by-step details for ECHO and DOTS disaster recovery, we request that FTA provide us its plans to address the business impact analysis of these two systems.

Regarding recommendation 9, FTA agreed to relocate backup equipment for ECHO and DOTS to utilize an existing DOT facility as the permanent alternate site for the two systems. However, we request that FTA provide us with an action plan for testing the disaster recovery processes for ECHO and DOTS.

ACTION REQUIRED

In accordance with DOT Order 8000.1C, we request that you clarify your response to recommendations 1, 8, and 9 and provide specific corrective action dates for all nine recommendations. We would appreciate receiving your written comments on this report within 30 days.

We appreciate the courtesies and cooperation of FTA and KPMG representatives. If you have questions concerning this report, please call me at (202) 366-1992 or Ted Alves, Assistant Inspector General for Financial and Information Technology Audits, at (202) 366-1496.

#

EXHIBIT A. SCOPE AND METHODOLOGY

Under contract with OIG, KPMG conducted an audit of computer security and controls for three information systems at FTA Headquarters and a contractor site in Herndon, Virginia. The audit covered fiscal year 2003 activities and was conducted from May to July 2003.

OIG and KPMG met to discuss the project scope and objectives. KPMG conducted the review based on an OIG-approved audit plan including interviews, reviews of documentation, observations of procedures, testing of control features, and scanning for network vulnerabilities.

OIG performed a quality assurance review of the KPMG audit work to determine compliance with applicable standards. Using a review guide provided by the President's Council on Integrity and Efficiency, we reviewed KPMG's audit program, conducted weekly status meetings with them to evaluate their progress, participated in meetings and briefings they had with FTA management, monitored their vulnerability testing, and reviewed their workpapers and audit findings. Based on our review, we determined KPMG conducted this audit in accordance with Government Auditing Standards prescribed by the Comptroller General of the United States, the General Accounting Office's Federal Information System Controls Audit Manual, and supplemental KPMG review guidelines.

KPMG

September 30, 2003

Mr. Kenneth Mead
U.S. Department of Transportation
Office of Inspector General
400 Seventh Street SW
Washington, D.C. 20590

Dear Mr. Mead:

KPMG LLP (KPMG) is pleased to submit this final report that summarizes our review of three Federal Transit Administration (FTA) systems supporting the grant award, administration and payment processes. KPMG LLP was contracted by the Office of Inspector General to conduct this review in support of the Fiscal Year (FY) 2003 financial statement audit required by the Chief Financial Officer's Act of 1990, as amended by the Government Management Reform Act of 1994.

Our review included evaluating controls over the Transportation Electronic Award Management System (TEAM), Electronic Clearing House Operation System (ECHO), and Delphi Online Transaction System (DOTS). We performed our review using guidance outlined in the General Accounting Office (GAO) Federal Information System Controls Audit Manual (FISCAM). We evaluated the controls over these systems from the period May 22, 2003 through July 31, 2003. The report describes the scope and objectives of our review as well as a detailed discussion of information technology concerns that the Federal Transit Administration (FTA) should address.

We appreciate the opportunity to provide information technology audit services to the Office of Inspector General and look forward to serving you in the future. Should you have any questions, please contact me at (202) 533-3024 or Geoffrey L. Weber, Senior Manager, at (202) 533-4344.

Very truly yours,

KPMG LLP

Attachment

Office of Inspector General

U.S. Department of Transportation

Federal Transit Administration
General Controls Review of the DOTS, ECHO and TEAM
Financial and Grant Management Systems

EXHIBIT B. KPMG AUDIT REPORT ON COMPUTER SECURITY AND CONTROLS OF FTA GRANT MANAGEMENT AND PAYMENT SYSTEMS

INTRODUCTION

The mission of the FTA is to support the goal of promoting the development and use of mass transit in the United States. The FTA is responsible for the administration of the program budget, the evaluation of grant applications for financial assistance, the grant award process, and oversight of transportation grants for mass transportation projects across the United States. During FY 2002, FTA disbursed over seven billion dollars to grantees for transit projects.

The Transportation Electronic Award Management System (TEAM) is the authoritative source for information concerning program budget execution, status of grant applications, awarded grant amounts and FTA dollar commitments. The Electronic Clearing House Operation System (ECHO) is used to process grantee draw down requests, totaling over seven billion dollars annually, and provides FTA Accounting with decision support over balances available and amounts. The Delphi Online Transaction System (DOTS) is FTA's reporting system, which is used to generate and customize financial reports.

Due to their criticality, the ability of the TEAM and ECHO systems to process and pay grants in a timely manner is essential to ensuring compliance with the requirements of the Cash Management Improvement Act of 1990. Additionally, the systems help to ensure compliance with the Anti-Deficiency Act by ensuring that payments do not exceed the established grant award amount.

This report presents the results of our audit of security controls over three Federal Transit Administration (FTA) systems that support the grant administration and payment processes. The integrity of these systems is important because they are the primary means of tracking and accounting for over seven billion dollars in FTA grants annually. We conducted this audit in support of the Fiscal Year (FY) 2003 financial statement audit as required by the Chief Financial Officer's Act of 1990, as amended by the Government Management Reform Act of 1994.

OBJECTIVES, SCOPE and METHODOLOGY

Our objectives were to evaluate the computer security and controls of three FTA systems used to approve, monitor, and pay grants for transportation projects. These systems include the TEAM, ECHO, and DOTS. The ECHO system is also utilized by the Federal Aviation Administration to support grant payments to airport authorities. The focus of our review was the entity-wide security program planning and management, access controls, network vulnerabilities, application software development and change controls, system software controls, segregation of duties, and service continuity.

Guidance for our review was provided from the General Accounting Office (GAO) Federal Information System Controls Audit Manual (FISCAM). Our approach for assessing the management and operational controls consisted of interviews with knowledgeable FTA personnel, policy and procedure review, selected system testing, and document analysis regarding specific control objectives that collectively constitute the minimum components of an effective information security program. The control objectives were drawn directly from long-standing requirements found in Federal law, DOT requirements, regulatory and technical criteria, and other Federal policy on security and privacy. Our approach for the assessment of the technical control areas focused on the System Administration Networking and Security (SANS) Top Twenty System Security Flaws, in addition to the Federal best practices. Network security software scans were performed at both the network level and host level and then analyzed for vulnerabilities.

RESULTS

We found weaknesses regarding the security program for DOTS, ECHO and TEAM:

- Weak security planning and management for FTA financial systems poses a risk that vulnerabilities may not be identified and corrected in a timely manner.
- Weak system access controls may lead to unauthorized usage of FTA financial systems.
- Weaknesses in the change control process for FTA financial systems may lead to erroneous or malicious code being introduced into the operating environment.
- Service continuity planning over FTA financial systems is not adequate to sustain operations in the event a service disruption occurs.

We provided summaries of individual weaknesses to FTA officials during the course of the audit. These officials generally agreed with the findings and committed to implementing the recommendations.

We conclude that these weaknesses represent deficiencies in the design or operation of the internal control structure, which could affect the FTA's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. While we did identify weaknesses, we did not find any evidence of fraud, abuse, or misuse within DOTS, ECHO or TEAM. Furthermore, we reviewed the payment process between the FTA and the grantee and no weaknesses were noted. However, our review procedures were not designed to specifically identify fraud, waste, and abuse. Instead, they were designed to identify potential control deficiencies that could lead to fraud, waste, and abuse.

- **Weak security planning and management for FTA financial systems poses a security risk**

The Certification & Accreditation (C&A) process includes operations that protect and defend information and systems by ensuring their confidentiality, integrity, and availability. Ensuring that appropriate security objectives are developed and that the security risks are identified and balanced against operational demands is a fundamental management responsibility. Weaknesses in this process create a risk that the systems will be vulnerable to unknown security weaknesses. Our review of planning documents showed that FTA did not properly address key requirements within DOT certification and accreditation guidance, such as requirements to conduct risk assessments, prepare security plans, and perform security tests and evaluations. To illustrate, FTA did not perform a security test and evaluation to accredit TEAM, which is a fundamental requirement of the certification and accreditation process. TEAM should not have been certified and accredited without this evaluation.

In addition, FTA employees and contractors have inadequate background checks and out–of-date position descriptions that do not describe any security responsibilities. We found that all ten financial systems contractors and one of five FTA administrator background checks that we reviewed were inadequate. In these cases, the background check performed by FTA was not sufficient to meet the position's sensitivity level. For example, one system administrator required a background investigation, but had a low-level fingerprint check.

These weaknesses exist because FTA management did not follow DOT guidelines for certification and accreditation, including specific requirements to perform a security test and evaluation of TEAM before accrediting the system. Also, FTA did not follow policy regarding personnel controls, such as DOT requirements for proper background investigations. Without adequate procedures regarding security planning and personnel controls, FTA could be unknowingly accepting high-risk vulnerabilities that could lead to fraud, loss, or unauthorized modification of data.

- Security Test & Evaluation (ST&E). An ST&E is a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. This is one of the fundamental requirements leading to a certification and accreditation. We found that a ST&E was not performed as part of the certification and accreditation process for the TEAM system. As a result, the TEAM system was accredited to operate without the results of a ST&E. By not performing a ST&E, management cannot have an understanding of the true status of controls in order to make a decision as to whether risks are properly mitigated or acceptable. Vulnerabilities documented in this report should have been identified during an adequately performed ST&E, prior to the certification and accreditation.

  FTA performed the ST&E for its financial systems by using a checklist of over 200 questions that was developed by the National Institute of Standards and Technology (NIST). Within this checklist for ECHO and DOTS, we identified at least ten steps in each document that were marked as passed, pending, or not applicable that, based on the detailed notes supporting those responses, should have failed. For example, the system ST&E calls for a review to determine whether the contingency plan is periodically tested, which is a critical component of security management. However, the ST&E results state that this item is pending, and the response is noted as not applicable even though testing has not been performed. Steps were missing when compared to the NIST checklist without an explanation. Furthermore, there was no supporting documentation available for any of the steps that were marked as having passed.

  Background checks. Background checks are important since they help to determine whether a particular individual is suitable for a given position. FTA employees and many contractors have inadequate background checks. We examined key IT management positions such as security officers, system administrators, database administrators, and system managers, and found that all ten contractors and one FTA employee we reviewed did not have the level of background checks required by DOT. These weaknesses are caused in part because the current process for tracking the background checks received by contactors and employees is unreliable. For example, we found that the FTA Human Resources security point of contact did not have the ability to identify the employees and contractors responsible for development, management, and security for TEAM, who required a security clearance.

	FTA Employees	Contractors
Number of Persons Reviewed	5	10
Adequate Background Check	4	0
Inadequate Background Check	1	10

- Risk Assessments. The purpose of each risk assessment is to identify all threats and vulnerabilities and the corresponding mitigating controls that will decrease their severity. Although risk assessments were performed for all three systems, the risk assessments were deficient. For example, we found that risk assessments for DOTS and TEAM did not address the existing potential vulnerability of the systems administrator or programmer making code changes to the system without management knowledge. Additionally, the DOTS risk assessment did not identify vulnerabilities for identified threats, the ECHO risk assessment only partially defined and did not describe the mitigating controls, and the TEAM risk assessment did not identify high-risk threats such as hackers and malicious software attacks. Without adequately completing the risk assessment, FTA could unknowingly be accepting high-risk vulnerabilities that could lead to fraud, loss, or unauthorized modification of data.

- Security Plan. The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. We noted weaknesses in the DOTS, ECHO, and TEAM security plans. We compared the security plans to DOT and National Institute of Standards and Technology (NIST) guidance and noted that many of the sections were either missing entirely or lacking required information. For example, in each of the plans, the rating of confidentiality, integrity, and availability is not made in accordance with the categories in the Departmental plan (Mission-critical, financial, budgetary, commercial, etc.) Security responsibilities and controls cannot be clearly identified and communicated to system managers and users without comprehensive, entity-wide security program plans. The lack of a complete plan may cause the FTA's information systems to be more susceptible to improper access, use, and/or loss of sensitive information.

Recommendations

1. Re-certify each financial system by reassessing each financial systems risk assessment and security plan and ensure that they comply with NIST and DOT guidance. Conduct a ST&E that complies with NIST guidance and ensure that the ST&E results are properly documented to support any tests deemed as passing.

2. Review FTA IT-related positions to identify staff and contractors who require background checks. Once complete, conduct the appropriate background check commensurate with the position's sensitivity.

- **Weak system access controls may lead to unauthorized usage of FTA financial systems**

Access controls are important because they restrict access to computer resources to personnel with a valid need and prevent unauthorized personnel from using the system. FTA management has not developed detailed polices and procedures to guide system administrators and the system owners to effectively grant, monitor, and terminate access, including physical access. The lack of a structured process to grant, monitor, and terminate user access increases the risk that unauthorized users may be able to create, modify, or delete financial data within the system or allow sabotage of equipment.

We found that two-thirds of FTA terminated employees during fiscal year 2003 were not removed in an timely manner, password controls for DOTS were not consistently enforced, and physical access to the DOTS and ECHO data center is not adequately controlled. Documentation supporting authorized user access and acknowledgement of the system rules of behavior regarding proper and prohibited conduct was also incomplete, making the monitoring and revalidation of employee access difficult to enforce.

The results of our vulnerability scanning showed five high and seven medium risks that need to be addressed for TEAM and DOTS. The five high and seven medium vulnerabilities existed because management did not ensure that certain parameters were enforced and that updated software versions and software patches were current. We were unable to conduct an analysis of ECHO due to the fact that the ECHO application is antiquated and the platform it operates on is outdated, which does not permit our scanning tools to analyze the system. Obsolescence may expose ECHO to security risks since third-party system support is not available.

- <u>Terminated employees.</u> User accounts for terminated FTA employees are not being removed from TEAM in a timely manner. We obtained a list of 22 employees who left the organization in FY 2003. Of those 22 user accounts associated with the terminated employees, 17 user accounts were not disabled immediately upon termination to prevent further access to the system. By not immediately removing access for separated employees, FTA faces increased exposure to malicious acts by disgruntled employees and increased risk of unauthorized access. We did note that once the information regarding the active accounts was provided to FTA, the active accounts were disabled.

- <u>User authorization.</u> User access forms that document authorized access levels were incomplete or not retained. For DOTS, user authorizations were not consistently required as only three out of seven users we sampled had the proper user access request forms. For ECHO, no documentation is maintained regarding the granted user access. For TEAM, we found instances where a standard user form and informal email requests were used. However, the standard form is inconsistently used and the email requests for authorizations to TEAM are not kept on file for the life of the account. Without a historical record of user account authorization forms, system administrators may not be able to determine if user access is valid and necessary.

- <u>Rules of Behavior.</u> "Rules of behavior" that document an acknowledgement of prohibited employee conduct were not always completed or retained. For DOTS, rules of behavior are used inconsistently as five out of the seven users we sampled did not have acknowledgement forms. With respect to TEAM, users are not being asked to complete a rules of behavior document before gaining access to this system. By not requiring users to sign rules of behavior before accessing a system, the risk exists that users may unwillingly divulge or compromise information due to a lack of security awareness and make it difficult to hold users accountable for their actions.

- Physical Access. The FTA is unable to determine whether the current DOTS and ECHO data center access list reflects a complete list of persons with access to the data center because (1) the list is not updated on a regular basis and (2) the cipher lock combination is not changed on a periodic basis. By not periodically updating the access list to the DOTS and ECHO data center, the FTA cannot have reasonable assurance about the personnel who are knowledgeable of the cipher lock combination, and thus, have access to the data center. Coupled with the fact that FTA cannot change the cipher lock combination since the key to do so is missing, no practical means exists to ensure access to the DOTS and ECHO data center is controlled.

- Vulnerability Assessment for FTA Financial Systems. We used a commercial scanning tool to evaluate logical access controls over the host platforms for the DOTS and TEAM systems. As a result of our internal scanning test work for the DOTS system, we identified five high risk and three medium risk vulnerabilities. We also identified four medium risk vulnerabilities related to the TEAM system platforms. These vulnerabilities present a potential opportunity for users to gain unauthorized access to the systems platforms and modify or destroy information. We shared our detailed results with FTA officials but did not describe them in this report because the details could allow the vulnerabilities to be exploited. However, we noted that FTA took the recommended corrective actions toward fixing the vulnerabilities identified.

  Commercial scanning tools are limited in their ability to audit and evaluate vulnerabilities on the ECHO platform because it is outdated. Inherent weaknesses exist due to the FTA's reliance on an obsolete system and telecommunications. The ECHO application lacks an automated systems management capability such as system-based audit logging. Due to the lack of system-based audit functionality for the ECHO system, no automated controls exist to ensure adequate oversight over data files and processing operations for ECHO. Additionally, FTA reliance on outdated software makes ECHO more difficult to maintain. Obsolete systems are reliant on the knowledge of key individuals and lack vendor/third-party support, system and security patch accessibility, and effective disaster recovery options, which increases FTA's risk of denial of service if malicious attacks or unforeseen events occur.

Recommendations

1. Develop procedures to periodically revalidate user access and to monitor security violations for all FTA financial systems. Procedures should include a process to terminate users in a timely and effective manner.

2. Document and monitor the user access process for the FTA financial systems and secure physical locations. For system access, this should entail the use of formal access request forms and rules of behavior for all users to complete before they access the system. These forms should be maintained for the period of time that the user account is active.

3. Implement the appropriate software versions, patches, and the necessary system parameters to prevent the high and medium risk vulnerabilities for the DOTS system.

4. Conduct a cost/benefit analysis to determine whether ECHO should be replaced or upgraded to a standard platform that will permit FTA management to audit and oversee system activities and security functions, and to obtain vendor/third-party support.

- **Weaknesses exist in the change control process for FTA financial systems.**

Without an adequate change control process, unauthorized personnel can load and execute software on a system, the system is more vulnerable to unexpected software interactions, and to software that may subvert or bypass security controls. We found a lack of segregation of duties in the FTA financial system change control process. For example, the ECHO system administrator is responsible for all aspects of the ECHO change control process with no management oversight of staff activities. For DOTS, ECHO, and TEAM, system changes are not thoroughly documented and the construction of test plans and documentation of test results are not developed. Testing around DOTS and ECHO modifications is also informal and not segregated, and is only conducted by one or a few individuals.

These weaknesses exist because FTA management has not complied with DOT and NIST guidance requiring adequate system change controls and segregation of duties. Lack of a formal, standardized change management process could result in unauthorized and/or inaccurate program changes being introduced into the system, which can lead to unplanned system downtime, fraud, abuse, corrupt data, or denial of service.

- Segregation of Duties. Segregation of Duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process. A lack of segregation of duties exists in the change control process between the development and implementation of software changes. For DOTS and ECHO, only the system administrator controls the change management process including system programming and code migration into the production environment. Although this is not his primary duty, we noted that the TEAM programmer also has the ability to upload code into the production environment.

- System Change Procedures. System development procedures and standards are key management controls. Lack of a formal, standardized, and authorized development processes could result in unauthorized and potentially malicious computer program changes being implemented into the production environment that could lead to corruption of data or system downtime. System changes are not sufficiently documented to support an audit trail and the construction of test plans and documentation of test results are not developed for FTA financial systems. Additionally, testing modifications are not formally documented and structured.

Recommendations

1. Review the existing roles and responsibilities for FTA IT staff, and develop and document a policy that identifies and segregates incompatible duties. Where duties cannot be properly segregated due to resource constraints, FTA management should institute compensating controls that include system audit logging and supervisory review of the activity on a periodic basis.

2. Develop policies and procedures that (1) detail the development and construction of test plans, document test results, deliver and implement software, and require approval by management for all financial applications, (2) govern who should have access to the financial system and code, and (3) implement a mechanism to track this access on a regular basis.

- **Service continuity planning is not adequate to sustain operations in the event a service disruption occurs.**

The FTA has not developed adequate contingency plans for its financial systems. First, the FTA has not conducted a business impact analysis (BIA), the fundamental first step in planning for contingencies. The existing contingency plans do not document procedures that provide accurate and detailed IT system backup and recovery if a disaster was to occur and the process has not been tested. In addition, key person dependencies exist that impact service continuity, with no backup personnel adequately trained to handle daily operations.

The FTA has not followed DOT and Federal guidance regarding service continuity. The FTA noted it has limited funding to dedicate toward service continuity issues such as providing necessary human resources to compensate for key dependencies. However, without proper contingency planning controls, the FTA exposes itself to an increased risk of service disruption and the possibility of not meeting mission requirements specified in the Cash Management Improvement Act of 1990.

- A Business Impact Analysis has not been performed. The BIA is a key step in the contingency planning process. The BIA is used to determine maximum allowable downtimes and appropriate response measures for systems as part of the contingency planning process, and enables the FTA to fully characterize the system requirements, processes, and interdependencies and use this information to determine contingency requirements and priorities for limited resources. We noted that none of the FTA financial systems had conducted this step prior to drafting their contingency plans.

- Contingency Plans. Contingency plans do not provide accurate and detailed data backup and recovery information, and the contingency plans have not been tested. Disaster recovery roles are not defined or described. Furthermore, no responsibilities or duties are documented for each role. There were no notification procedures or contact information for the key personnel involved with disaster recovery. Detailed procedures regarding the backup, recovery, and restoration of FTA financial systems are not documented. Although FTA states that hotsite facilities at Computer Associates, Inc. exist for DOTS and ECHO, the DOTS backup hardware currently resides at the primary processing site. While ECHO equipment is located at the alternate processing site, it does not include all of the hardware necessary to restore operations. Additionally, the disaster recovery facility for DOTS, ECHO, and TEAM are approximately 25 miles apart and may not be adequately separated in case of a large scale disaster affecting the entire geographical region.

- Personnel Continuity and Knowledge Management. Dependencies exist that impact service continuity. DOTS and TEAM rely on contractors to perform the day-to-day management of these systems including data backup and contingency planning. This creates a dependency for FTA. Without adequate documentation regarding data backup and disaster recovery procedures, the FTA risks losing its system operations knowledge base if these contracts are not renewed, are prematurely terminated, or if the individuals cease to work for their contract employer. For ECHO, the system administrator is responsible for various aspects of system operations including system administration, change management and access control. No trained backup exists to assume these duties in the event the system administrator is unavailable.

Recommendations

1. Conduct a BIA as a part of the contingency planning process. The BIA should consider the critical resources, the maximum allowable outage, the measured impact, and the recovery strategy. Additionally, as part of the BIA recovery strategy, as well as part of the risk assessment, FTA should consider safeguards for service continuity that take into account geographical location to minimize threats occurring simultaneously at both the primary location and the disaster recovery site.

2. Document backup and disaster recovery procedures that include personnel roles and emergency notification. The procedures should detail step-by-step processes that personnel, with a reasonable system understanding and IT background, can use to reestablish continuity of service when disruptions occur.

3. Test the backup and disaster recovery processes to ensure that FTA management and other critical parties understand their recovery roles and responsibilities, and that the system can be restored as planned.

4. Designate personnel, with a reasonable ECHO system understanding and IT background, to serve in a backup capacity. Properly document contractor day-to-day activities and operating procedures for DOTS and TEAM.

Memorandum

U.S. Department
of Transportation
Federal Transit Administration

Subject: INFORMATION: Response to Draft Report on Computer Security and Controls of Grant Management and Payment Systems

Date:

From: Susan Knisely
Senior Director, Office of Transit Safety
and Security

Reply to
Attn. of:

To: Theodore P. Alves
Assistant Inspector General for Financial
and Information Technology Audits

The Federal Transit Administration (FTA) has reviewed the Office of Inspector General (OIG) Draft Report on Computer Security and Controls of Grant Management and Payment Systems; Project No. 03F3012F000.

In general, FTA concurs with the report recommendations. The following are FTA's comments that address specific actions taken and include target dates for planned actions to implement the recommendations.

OIG recommends that FTA:

1. Test and evaluate security controls in TEAM, ECHO and DOTS and develop more comprehensive risk assessments and security plans for all three systems.

FTA Comment

FTA agrees with the OIG recommendation. The last risk assessment for TEAM-Web system was completed in September 2001 as part of the fiscal year 2002 system Certification and Accreditation process. FTA is required to repeat this process for fiscal year 2005 operations. FTA will request funding, complete a more comprehensive risk assessment and update the security plans for the fiscal year 2005 TEAM-Web Certification and Accreditation process.

FTA has modified the security plan for ECHO and DOTS to include the identified missing elements and developed a process to assess completeness. In addition, the safeguards and vulnerabilities have been incorporated into the risk assessments. Additional funding has been requested for FY 2004 to cover the costs associated with more comprehensive risk assessments and security plans for these systems.

2. Complete the appropriate background checks on the Federal and contractor employees KPMG identified.

FTA Comment

FTA agrees with the OIG recommendation. FTA will work with their Human Resources Office to get a current status of background investigations for individuals cited in the audit report and to determine the level in which the investigations need to be raised to meet the OIG recommendations in this area. Also, additional funding has been requested for FY 2004 to cover the costs associated with the higher levels of background investigations.

3. Develop procedures for granting, removing, and periodically revalidating user access, and enforce use of access request forms and security agreements (Rules of Behavior) before granting system access.

FTA Comment

FTA agrees with the OIG recommendation. FTA has developed and implemented new procedures for removing users. This process is using the TEAM-Web change management database to record all employee removal requests. The change management system will notify key TEAM-Web help desk staff if the removal has not been accomplished on the day of separation. The transactions for the new process come from the FTA employee tracking system. FTA plans to install an automated procedure to allow users to sign/attest the "Rules of Behavior" statement at logon. FTA plans to put this procedure in place for the fiscal year 2004 operations.

FTA will implement a policy for ECHO and DOTS requiring all users of these systems to return a signed "Rules of Behavior" that acknowledges the users' responsibilities for using the systems. Users who do not return a "signed" Rules of Behavior document within a prescribed period will automatically have their user accounts disabled until such time the document is received. This procedure will be implemented beginning FY 2004.

4. Regularly scan FTA financial system computers for vulnerabilities and timely install software patches provided by the manufactures or reconfigure software settings.

FTA Comment

FTA agrees with the OIG recommendation. The TEAM-Web software patches are tracked using the Change Management System, and the server checklist process. There was one non-critical patch not applied at the time of the audit. This has been corrected and procedures are in place to apply non-critical patches weekly. Critical patches have always been applied immediately. FTA has placed a request in the Office of Information Technology change management system to include the TEAM-Web servers in the Departmental "Found Stone Found Scan" process. This is a high priority request and the tracking number is 812. Once implemented, the TEAM –Web servers will be scanned weekly.

The DOTS patches have been applied on a regular basis with the exception of a later version of Secure Sockets Layer (SSL), which is needed to restrict client access. The existing version has been taken off-line and the new version is being shipped and will be installed upon receipt. Since ECHO currently utilizes obsolete software, FTA plans to migrate it to another platform that has a more secure environment during FY 2004.

5. Enhance physical access controls over the ECHO and DOTS computer room by maintaining a list of individuals authorized to enter the data center and changing the combination to the lock on a periodic basis.

FTA Comment

FTA agrees with the OIG recommendation. FTA has installed a logbook on the computer room door requiring all staff to sign in and out when entering the computer room. In addition, only the Financial Systems staff has access to the code for entry and must be contacted to provide entry. The Administrative Services office is making arrangements with the locksmith to change the cipher lock and a master key will be provided for use as a backup.

6. Increase management oversight of, and develop documented procedures for, ECHO system maintenance work.

FTA Comment

FTA agrees with the OIG recommendation. FTA originally established a Systems Maintenance Manual for the ECHO system which covered the functional roles and responsibilities for the system. However, the document was not kept updated to reflect the existing configuration. FTA will develop and document an ECHO System Administrator manual to include specific security and operating procedures related to the systems administrator's day-to-day activities and role.

7. Require that test plans, test results, and user approvals for ECHO and DOTS system changes be documented.

FTA Comment

FTA agrees with the OIG recommendation. FTA has developed policies and procedures that detail the development and construction of test plans, documentation of test results, delivery and implementation of software and approval by management for all system and application software for DOTS. ECHO software is obsolete and applications will be migrated to a web-based and Oracle environment in FY 2004. The Financial Systems Office staff has implemented a software application to support configuration management activities in monitoring and tracking all work and system change requests.

8. Enhance the contingency plans with a business impact analysis and detailed disaster recovery procedures including personnel roles and emergency notifications for all three systems.

FTA Comment

FTA agrees with the OIG recommendation. FTA will include a business impact analysis in the TEAM-Web disaster recovery plan. The existing TEAM disaster recovery process includes roles and emergency notification procedures. These procedures were used during the last hurricane "Isabel." The TEAM-Web system was up and operational for the entire period of the hurricane disaster that closed the Federal government.

FTA will perform a Security Test and Evaluation (ST&E) process that complies with NIST 800-26 and properly document the results for ECHO and DOTS. FTA also will document the disaster recovery procedures to include step-by-step details for setting up the hardware, software and telecommunications connectivity.

9. Test disaster recovery processes for ECHO and DOTS, and determine whether the recovery site is distant enough to ensure continued operations in case of large-scale disasters.

FTA Comment

FTA agrees with the OIG recommendation. FTA has designated a DOT facility as the interim hotsite for both ECHO and DOTS. The backup equipment for ECHO has been relocated to this facility, and the backup equipment for DOTS has been ordered and will be relocated upon receipt by FTA. Additional funding has been requested to complete the connectivity and other requirements identified to convert the offsite facility to a hotsite. FTA plans to utilize the Department of Transportation's (OST) COOP site.